

Confidential I – Voting System

¹Kaviranjani G, ²Anitha K

^{1,2}B.Tech. ISDF

^{1,2}Department of CSE,

^{1,2}Dr. MGR Educational and Research Institute, Chennai, India

Abstract— this project “CONFIDENTIAL I-VOTING SYSTEM” aims at making the voting process easy in all type of elections. This type of voting process provides non profitability sample of the participants to self-elect into participation. The term poling includes the terms such as call-in, mail-in, and some online polls. Before 1990’s the voting was performed using ballot paper and all the counting is done manually, hence it consumes a lot of time to make the final decision. There can be possibility of invalid votes, fake votes etc. And we switched that method of practicing by replacing the ballot papers to EVM (Electronic voting Machine). Here the EVM’s can be set up only in those particular wards, there comes another issue not all voters will be available during the time of election at the particular wards. This will affect the results while selecting the leader. All these make election a tedious task. In recent times in India, during the election the second wave of COVID transmission also made huge loss of human lives. And also, in any type of voting there will be a problem of fake voting. To avoid all these conflicts in our proposed system we are doing all the voting and counting with the help of computer through internet. It is the most efficient way to save the time of the person who is not available during the time of election at the particular wards. It makes the election process easy. It also avoids the process of physical touching or visiting any places and even during pandemic it will be more helpful to conduct elections. The system allows the user to vote for the candidate online. All the records of the candidate will also be available in the webpage which will help the voters to know about the candidate even if they are not aware of them. In present existing system there are lot of conflicts to overcome the drawbacks we made the whole system using block chain to provide more security to the system. This particular system was proposed to mark our work much easier and to reduce wastage of time. So, there is a need for the Confidential I-Voting System.

Keywords—*ballot paper, confidential voting, EVM, block chain*

I. INTRODUCTION

BACKGROUD INFORMATION:

In traditional times during elections, a voter usually goes to the voting booths. After one-on-one person confirmation with some IDs, the voter will get the permission to vote. Then the voter will be provided ballot paper which will help them to register the vote. Only once the ballot is used; it cannot be used for another time. However, this ballot must also be unidentified. The ballot must identify the voter who is authorized to vote, but it is not supposed to reveal their actual identity, and the voter must be given guarantee of this. Traditional polling methods had lots of trust issues among parties during the election. Advertisement of electronic voting, especially Internet voting, make a number of debates in favor of its implementation. They are linked to technology, social problems and election management. At first, electronic voting has the possible way to make the voting process easier and more easily available for the electors. This is especially right for improbable Internet voting and telephone voting than giving ballots, because it can be performed from any computer with an active Internet connection or any working telephone.

These latest methods are considerably lower the cost of voting because we can have the minimal setup for the booths. And for many electors there may be more entry points from which they are allowed to vote. There is the prospective to remove long queue at polling stations and it is better address accessibility problems for persons who are differently able, and those who are troubling from illness, those serving in the military or living abroad, those away on personal travel etc. And it is easily available for the single parents who may find it difficult to visit a traditional polling station leaving their kid.

ANALYSIS:

Online voting systems that has more advantages when compared with other voting techniques. It involves any one of the following steps in the setup such as distributing, voting, collecting and counting of ballots. Disadvantage exist and it includes potential flaws or weakness.

Online voting systems use votes to store in Computer memory. These ballots are used for no risk of exhausting the supply of ballots. In addition to that this type will remove the need for printing of paper ballots, a significant cost. Even it has advantages we will have an argument when it is comes to the cost of software validation, compiler trust validation, installation validation, delivery validation and validation of other steps related to electronic voting is complex and expensive.

- **Accessibility**

Online voting can be made fully accessible for persons with disabilities and for the people who can't vote in person. We can easily sit and our place to give our vote however there comes an issue for visually challenged peoples. Other than this we can simply login and register our vote.

- **Cryptographic verification**

The concept of election verifiability through cryptographic solutions will be effective in case of transparency and trust in online voting systems. It allows voters and election observers to verify that votes have been recorded, tallied and declared correctly, in a manner independent from the hardware and software running the election. There are three aspects of verifiability are considered. They are Individual verifiability allows a voter to check that our own vote is included in the election outcome, universal verifiability allows voters or election observers to check that the election outcome corresponds to the votes cast, and eligibility verifiability allows voters and voters to check that each vote in the election outcome was cast by a uniquely registered voter.

- **Voter intent**

Online voting able to provide immediate feedback to the voter detecting such possible problems as under voting and over voting which may result in an unordered result. This immediate feedback can be helpful in successfully determining voters' intent.

- **Audit trails**

A fundamental challenge of voting is to provide evidence that the votes were recorded as cast and they are being tabulated as recorded. Election results produced by voting systems that rely on voter-marked paper ballots can be verified with manual hand. The systems can include the ability for voters to verify how their votes were cast or enable officials to verify that votes were tabulated correctly.

PROBLEM STATEMENT:

The main problem that is faced by the current voting system is that people are subjected themselves to go to vote in the particular place of registration. Not all the people will be available at the time of the election. This creates a big issue while evaluating the results. The result will be varied because of the person who doesn't vote.

Another problem that is faced here is the fake vote. Because of the fake vote big impact is being created during the finalization of the leader in the country.

The time taken to count the result is also more so the results are declared later. This will lead the problem of changing of EVM's etc.

OBJECTIVE:

The main aim of the project of "CONFIDENTIAL I-VOTING SYSTEM" is to provide the basic fundamental rights for the human through various objectives-

- i. Maintain Confidentiality by not leaking the information to others and maintain the secrecy of the details of the voters.
- ii. All these information is encrypted properly to avoid the cyber-attacks as all these data will be collected, stored in the web page.
- iii. Proper authentication and Authorization is given for the users who logs in through our webpage.
- iv. People should get easily accessed once the internet connection is available.

SCOPE OF STUDY:

Our project focuses on the people intent of voting in the elections by

- Less effort and less labor intensive, as the primary cost and focus primary on creating, managing, and running a secure web voting portal.
- Increasing the number of voters as individuals will find it easier and more convenient to vote, especially those abroad.

II. LITERATURE SURVEY:

1. In **Khann** (2020) propose a way to eliminate the problematic aspects of conventional elections by using block chain technology. This paper gives the establishment of decentralized e-voting methodology rather than a centralized one through block chain technology and it is readily available voting mechanism that gives guaranty for the security of voters' identification and data transmission through verification. The proposed system uses several technologies, which includes ganache, truffle framework, and meta mask. The limitations of this system are that while casting vote it is visible, and it does not provide openness to the voters.
2. **Boshri** Suggested block chain-based democratic process. It is based on the Ethereum network (Bosri., 2019). The electoral commission of India has established an Ethereum account that holds voter data in this approach. Those voters who do not have access to smartphones they can cast their votes at a designated polling location. But instead of that they have to complete a biometric verification procedure before giving vote at the polling booth. Even after the usage of block chain it has many infoldments that are related to the third party in this system. Only the casted vote is recorded in the chain, which is added by a third party (Kumari 2020). Here in this case, the false vote is possible. Election administrators has to manage the lifecycle of an election.
3. An electronic voting system is presented in **Hjálmarsson** (2018) Here also block chain is used as a service to create a distributed electronic voting system. This proposed system has two types of nodes: district node and also a boot node. The district node indicates each voting district, and each district node is equipped with a software application that connects with the boot node. A boot node allows district nodes to identify and connect. This system cannot protect voters' privacy very well (Qu et al., 2020, Tso et al., 2019, Roh and Lee, 2020) and it doesn't consider self-tallying process (Fan 2019).
4. In **Jorge Lopes** (2019), they propose a block chain-based e-voting system using smart contracts. There are three categories of people who can communicate with the program, including the director, the developer, and the voter. Record, Creator, and Election are three contracts. The whole recording of contracts are responsible for storing voter who register their information to verify

authentication. After authentication, the application transfers a transfer fund to the Creator Contract who is responsible for the establishment of new Election Contract. An Election contract is created here, and it will send its address to the Creator Contract for vote to cast. Before being added to the block chain, the vote is being encrypted via homomorphic encryption, which is a kind of symmetric encryption.

5. In **Shahzad** (2019), the framework proposed in this system is an improved form of e-voting using block chain. The proof of completeness algorithm will deal with the development of blocks, the locking of blocks, the information management, and the design of a block chain, especially for the voting machines network. In the case of the formation of a block, the presiding officer (PO) shall verify the elector's unique identification and biometric authentication. Here in the proposed system the voter casts his vote, and then it is carried forward by the machine which produces a hash using SHA-256 and it will send the data to the presiding officer which is responsible to produce a block. The key downside of this strategy which requires more security, high privacy, and more transparency than others before it can be considered to be fully trustworthy voting method (Toapanta 2019).
6. In **Dagher** (2018) Bronco Vote, a block chain-based voting technology is developed to preserve voter anonymity and improve transparency while maintaining an open, safe, and cost-effective voting mechanism. Bronco Vote introduces a voting system utilizing block chain and smart contracts and Ethereum to obtain election administration and auditable election results for university environments. Three contracts were used in this system: Registrar, Creator, and Voting Contract. The limitations of this system are that it has a poorly protected method of registration and a weak voter authentication. Privacy concerns in the process are also present when it comes to the execution of the project.
7. **Li et al.** (2021) created and built AMV chain, an efficient and scalable voting system that uses block chain and smart contracts to provide transparent and decentralized voting. They starts by examining the flaws and problems that is being created in existing block chain-based voting systems, then review vital research to address these issues. Based on the specifications that is created for a reliable and efficient electronic voting system. Ring signatures which are linkable and gives the definitions are used in the voting process to break the link that is created between voters and votes which ensures voter anonymity.

III. AIM AND SCOPE OF PRESENT INVESTIGATION:

SECURITY ISSUES OF ONLINE VOTING:

Foreign experience revealed that they are often confronted by security issues while the online voting system is running. The initiation of any security issues that occurs was due to not only outsider (such as voters and attackers) but also it can happen because of insider (such as system developers and administrators), even just because the inheritance of some objects in the source code that are unsuitable. These errors that are caused the voting system may lead the system to crash. The solutions that are proposed here will correspondingly outlined and it will hold back the attacks that are caused while execution of the code. For example, to avoid hacker making intrusion during the voting system through network, we can design our proposed system that transmit data without the usage of network. Another example is to limit voter to input particular data by doing that we can prevent the command injection from running.

PROPOSED SYSTEM:

To avoid all these conflicts in our proposed system we are providing the I-voting which is basically an online voting page that is developed by using block chain technology. The user will register with their personal details. Once they complete the registration, they will login with the user credentials which they have been provided while registering. An OTP will be sent to the user mobile number or to the email ID, then only the user will be able to login into the system. All the candidates name and description had been given default in the page. The voters will login to the page and they will choose the person whom they want to vote. We have created the whole project using Django framework. And for the security purpose we are using the block chain technology.

IV EXPERIMENTAL OR MATERIAL AND METHOD:

The proposed voting mechanism includes four phases:

1. *First Phase: Registration Phase*

The First phase of our proposed system consists of Registration phase which has two parts:

- (i) Voter's registration
- (ii) Candidate Registration

Voter Registration - People who have the right to vote and are registered to vote in their local election district are called voters. The Election Commission which has the responsibility of providing and maintaining an up-to-date list of registered voters. As a result of that, each and every eligible voter in the particular place should visit their local voter registration center and provide the necessary information in order to claim them to be recognized as a genuine voter. It is the first stage in the system and is needed as part of the identity verification phase in keeping a track of which individuals have casted vote. It has to be served as a control mechanism that prevents unregistered individuals from being participating in the election by preventing them from casting of ballot.

2. *Second Phase: Voting Setup Phase*

This phase is divided into three parts:

- (i) Create Election
- (ii) Active Election

Create Election The election that is created by EC which joins Block chain using pair of keys that are public keys and private keys. After that it sends a transaction to the registration contract with a vote coin, starting and ending time.

3. **Third Phase: Voting Phase**

This phase is divided into two parts:

- (i) Voter Authentication
- (ii) Vote Casting

Voter Authentication - The Voter contract is in charge of the voter authentication procedure. All the voters must first sign in into their wallets using the private key to complete the whole authentication procedure. After that step, the voter should enter their credentials that has been given for authentication. In this case, the voter contract receives the credentials and generates a hash value from them to compare the hash value with other hash values already present in the block chain. If both hash values are found equal, the voter is valid for voting.

Vote Casting - In many ways, the block chain-based voting mechanism we're proposing is analogous to the concept of digital wallets. Each and every participant is given a digital wallet by the authority after the registration during the registration phase. In this proposed system, voting is made as a transaction that contains a transaction index, timestamp, vote for the chosen candidate, and transaction hash. After performing the complete authentication process, the voter can cast a vote. After the authentication procedure is completed, the voter receives a ballot containing a list of candidates with a party symbol. Voters can select candidates from the list of candidates and vote using the vote coin. Then the voter will get their vote id like the candidate id. Then the casted vote is encrypted using the election commissioner's public key and saved on the block chain.

4. **Fourth Phase: Result Phase**

This phase consists of:

- (i) Vote Counting Unit
- (ii) Publish Result

Vote Counting Unit - EC enters the private key into the system as part of the counting procedure. Each EBi will be decrypted, and the voting contract will transfer the voting currency to the public key of each of the candidates who have been chosen. Through the path of candidate contract, once the coin delivered, the vote is locked soon after receiving it. It is equivalent of determining the amount of money owned by a specific address. In the end, the number of coins in each candidate's wallet represents the number of votes cast on him.

Publish Result - After voting, every vote will form a block and add it to the chain. The vote will be counted instantaneously after the vote is submitted, as there will be no risk of vote tampering and vote manipulation. The winner is found by checking the account of the candidate. Then a list is made, which contains a region, seat number, candidates obtained the vote, and winner of that region. The total votes of each candidate and the winning candidate are noted and they are verified. Then the final result is published in the result panel.

Candidate Registration - Since a candidate is also a voter here, the candidate registration procedure will be similar to voter registration. They must complete several additional steps following key generating in order to be considered a candidate.

IMPLEMENTATION

To provide more security to the websites we choose to develop and work our software on the basis of **BLOCKCHAIN**.

The application is divided into basically two sides:

1. Server-side
2. Client-side

Server-side:

On the server side, the block chain network is running. The server-side components used are:

1. **Ganache** - It is used for managing and testing the application at the local machine. Ganache is a specific RPC Server that can be checked and built for Truffle, which is accessible as a mobile and commands line application. It can be used at any point in the development process while it allows us to update, reuse, and test our App in a safe and secure manner. It is a tool that allows us to run Block chain locally and perform tests, issue commands, and observe the status of the Block chain. It's a block chain simulator that's been installed locally. Ganache uses a graphical interface to simulate Block chain networks and Live-test Smart Contracts without the use of virtual test networks or a remote network.

2. **Django** - It is a popular Python web framework that facilitates quick web design and development. It is a free-to-use framework which enables developers to reuse code to build high-quality web apps and APIs. It also helps to avoid security blunders and supports data driven architecture and moves software from concept to launch quickly.

3. **Python** - Python is secure, scalable and easy to use language. The whole block chain project can be compiled under three major components - Voters - They are the one who register their personal details and who cast the votes. They act as a client in this project when writing the code because they are considered as both voters and candidates in this case. So, we will create a client class in our code that has the ability to participate as voters and also as a candidate. Admin - The admin is the one who picks up the transactions from a transaction pool and assembles them in a block. They will note each and every progress that is being happening in the voting process.

4. Block chain - Finally, a Block chain is a data structure that will create private keys and public keys. Both keys will be changed for every node. That is the reason we chose this concept of block chain in our project because it is very secure.

5. MySQL - It is used as a mode of communication between client and server. We used MySQL for the storage because of following features like performance of database in maintaining enormous amount of data, its high availability where they can easily facilitate data over many servers and for the security, they provide like user account authorization etc.

Client-side:

On the client side the components used are:

HTML & CSS - We used HTML and CSS to create client side. We combined these two because they are easy to learn and easy to use. HTML allows us to build the structure of the website and CSS allows to run the website.

V RESULTS AND DISSCUSSION:

The proper working of the project is based on the testing that are done-

To get the desired result we have done following testing. They are

SQL INJECTION:

Even after developing our project in block chain there is the possibility of SQL injection attack to happen, because we have the candidate registration page which is easily prone to SQL injection type of attack when not coded properly. So to avoid that while coding algorithm itself we used the code that avoids unwanted symbols and commands that will connect to the database.

```
def is_admin(username: str):
    with connection.cursor() as cursor:
        cursor.execute("""
SELECT
    Admin
FROM
    Users
WHERE
    Username + %(username)s
    """, {
    'username': username
    })
    result= cursor.fetchone()
if result is None:
    #User does not exist
Return false

    Admin, = result
    Return admin
```

SYSTEM TESTING:

Software testing is a critical element of software quality assurance and gives review of specification, design, and coding. The user tests the developed system and changes are made according to their needs. The testing phase implementation that is aimed at assuring at the system works accurately and efficiently. Testing is vital to the success of the system. System testing makes a logical assumption that if all the parts of the system are correct, the goal will be successfully achieved. The system of the candidate is subjected to a variety of tests such as recover, security and usability tests. A series of testing is performed for the proposed system before the system is ready for the user acceptance testing. The system test should involve all the elements that compose the system including program validation checking, files, and forms and triggers procedures.

UNIT TESTING

Unit testing focuses on the effort of the smallest unit of software design of the module. This is also known as 'Module Testing. The module of this project is tested separately. This testing was carried out during programming stage itself in this testing each module is found to be working satisfactorily with regards to the expected output from the module.

VALIDATING TESTING

Here the software is completely assembled as a package, interfacing errors have been uncovered and corrected and final series of software test begins. Validation succeeds when the software function in a manner that can be reasonably expected by the customer.

OTP VERIFICATION:

The usage of block chain in our proposed system is secure. On top of that we were using OTP verification for the users who are logging in. This will create a strong barrier for the unwanted authorizations. This will provide additional security to the user because without the completing this OTP verification phase user is not able to login and cast the vote for the system.

VI SUMMARY AND CONCLUSION:**PROJECT SUMMARY AND LIMITATIONS:**

Till today only little country uses this type of online voting. Big democratic countries like India are still in the EVM type voting. Though this project is created in the block chain and is secure and for authentication we can use MFA to give proper authentication for the registered candidates.

CONCLUSION

In the project of “**CONFIDENTIAL E-VOTING SYSTEM**” we will manage the Voter’s information by which voter can login and use his voting rights. The system will incorporate all features of voting system. It provides the tools for maintaining voter’s vote to every party and it count total no. of votes of every party. There is a DATABASE which is maintained by the ELECTION COMMISSION OF INDIA in which all the names of voter with complete information are stored. In this user who is above 18 years’ register his/her information on the database and when he/she want to vote he/she has to login by his id and password and can vote to any party only single time. Voting detail store in database and the result is displayed by calculation. By online voting system percentage of voting is increases. It decreases the cost and time of voting process. It is very easy to use and it is varying less time consuming. It is very easy to debug. How securely we can conduct an election in flawless manner without any issues. The problems that are faced by the present system has been resolved and the more secure way for voting has been brought with the help of the project.

VII REFERENCES:

- [1] Chiara Braghin, Stelvio Cimato, Simone Cominesi, Ernesto Damiani, and Lara Mauri. Towards Block chain-Based E-Voting Systems, pages 274–286. 12 2019. ISBN 978-3-030-36690-2.
- [2] José Luís Pereira Jorge Lopes. Block chain based e-voting system: A proposal. In Twenty-fifth Americas Conference on Information Systems, Cancun, 2019, 2019. Umair Khalid, Muhammad Asim, Thar Baker, Patrick Hung, Muhammad Adnan Tariq, and Laura Rafferty. A decentralized lightweight block chain-based authentication mechanism for iot systems. Cluster Computing, 23, 09 2020. Saad Moin Khan, Aansa Arshad, Gazala Mushtaq, Aqeel Khalique, and Tarek Husein. Implementation of decentralized block chain e-voting. EAI Endorsed Transactions on Smart Cities, 4 (10), 6 2020.
- [3] Chenchen Li, Jiang Xiao, Xiaohai Dai, and Hai Jin. Amvchain: authority management mechanism on block chain-based voting systems. Peer-to-peer networking and Applications, pages 1–12, 2021.
- [4] B. Rogers, S. Chhabra, M. Prvulovic, and Y. Solihin. Using address independent seed encryption and bonsai merkle trees to make secure processors os- and performance-friendly. In 40th Annual IEEE/ACM International Symposium on Microarchitecture (MICRO 2007), pages 183–196, 2007. Chang-Hyun Roh* and Im-Yeong Lee**. A study on electronic voting system using private block chain. JOURNAL OF INFORMATION PROCESSING SYSTEMS, 16, 04 2020.
- [5] Samarth Shakya and Vivek Kapoor. A decentralized polling system using ethereum technology. Journal of Information Technology Management, 14 (Security and Resource Management challenges for Internet of Things): 1–8, 2022.